UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF	)	
COMPUTER SERVERS AND RECORDS	)	Case No.: 18-mj-234-01-AJ
OF MICROSOFT INCORPORATED FOR	)	
INFORMATION ASSOCIATED WITH	)	
THE E-MAIL ACCOUNTS	)	UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, BRENDAN M. QUINLAN, being first duly sworn, hereby state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent employed by the Office of Export Enforcement (OEE), Bureau of Industry and Security ("BIS"), of the United States Department of Commerce. I have been employed as a Special Agent with the United States Department of Commerce since November 2016, and before that was a Special Agent with the Department of State, Diplomatic Security Service beginning in March 2010. Prior to that, I was an Immigration Enforcement Agent with the United States Department of Homeland Security for approximately three years. I am authorized to make arrests for violations of federal law and I am familiar with the means by which individuals use computers and information networks to commit various crimes.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the individuals and entities listed below, and others, are violating the International Emergency Economic Powers Act, in violation of 50 U.S.C. §§ 1702 and 1705, by exporting U.S.-origin goods to the Advanced Engineering Research Organization (AERO), an entity in Pakistan currently on the Bureau of Industry and Security Entity List, and as such, denied from receiving such goods. Their activities are also violations of 13 U.S.C. § 305 (unlawful export information activities), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 554 (outbound smuggling), 18

U.S.C. § 1001 (false statements), and 18 U.S.C. § 1956 (money laundering) (further referred to as the "Subject Offenses.")

3. The individuals and entities listed below, as well as their last known addresses, constitute a procurement network that exists to acquire U.S.-origin commodities for AERO in violation of the Subject Offenses:

a. Haji Wali Muhammad Shiekh, Mississauga, Ontario, Canada

b. Muhammad Wali, Mississauga, Ontario, Canada

c. Kamran Wali, Rawalpindi, Punjab, Pakistan

d. Jason Gao, Kowloon, Hong Kong

e. M.A. Khan, Kowloon, Hong Kong

f. Waheed Ahmed, Essex, UK

g. Shamsa Ahmed, Essex, UK

h. Hina Iqbal, Oak Field House, Essex, United Kingdom

i. Rana Tanveer, Beckley, WV

j. Buziness World, 4453 Weeping Willow Drive, Mississauga, Ontario, Canada

k. Business World, 2nd Floor, Kau On Building, 251-253 Cheung Sha Wan Road, Kowloon, Hong Kong

l. Industria HK Ltd, 2nd Floor, Kau On Building, 251-253 Cheung Sha Wan Road,

Kowloon, Hong Kong

m. Transcool Auto Air Conditioning, 2nd Floor, Kau On Building, 251-253 Cheung Sha Wan Road, Kowloon, Hong Kong

n. Business World, 1st Floor, Jahanzeb Center, Bank Road, Saddar, Rawalpindi, Punjab, Pakistan

o. Product Engineering, Unit 10, Chowk Gowalmandi, Daryabad, Gowalmandi, Rawalpindi, Punjab, Pakistan

p. Business International GB, Oak Field House, 3 Oak Field Road Ilford Essex, United Kingdom

q. Industria GB 109 Rose Lane in Romford, UK

r. Industria, Inc., 205 Prince Street, Beckley, WV

4. I submit this affidavit in support of an application for a warrant under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of Criminal Procedure to search and seize records and data from the e-mail accounts identified as bz @hotmail.com (TA1) and an @hotmail.com. (TA2) ("the Target Accounts") (as described in Attachment A).

5. I have probable cause to believe that these accounts contain evidence, fruits, and instrumentalities of the crimes identified above, as described in Attachment B.

6. Based on the e-mail addresses' domain name, I have probable cause to believe that the accounts and relevant data are maintained by Microsoft, Inc., which government databases indicate, accepts service of process at 1025 La Avenida, Mountain View, California, as described in Attachment A.

7. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses.

This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

RELEVANT LAW

8. Under the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1707, the President of the United States was granted authority to deal with unusual and extraordinary threats to the national security, foreign policy, or economy of the United States. 50 U.S.C. § 1701(a). Pursuant to that authority, the President may declare a national emergency through Executive Orders that have the full force and effect of law. Among other things, IEEPA empowers the President to issue regulations governing exports from the United States.

9. On September 18, 2014, acting under the authority of IEEPA, the multi-agency body known as the End-user Review Committee (ERC) "determined to add Pakistan's Advanced Engineering Research Organization (AERO) and entities working with AERO to the Entity List for their involvement in activities contrary to the national security and foreign policy interests of the United States related to the illicit export, reexport and transfer (in-country) of items subject to the EAR to unauthorized end users in Pakistan as described in § 744.11(b)(5) of the Export Administration Regulations (EAR, 15 CFR §§730-774). These entities' involvement in the procurement of sensitive U.S. technology in support of Pakistan's development of its missile and strategic unmanned aerial vehicle (UAV) programs is in violation of § 744.3 of the EAR, which requires a license to export, reexport or transfer (in-country) any item subject to the EAR that the exporter, reexporter, or in-country transferor knows will be used in the design, development, production or use of rocket systems by a country listed in the EAR's Country Group D:4 in

Supplement No. 1 to part 740, in which Pakistan is included."[1] The EAR referenced in this publication is the Export Administration Regulations, which are Title 15 of the Code of Federal Regulations, Parts 730-774.

10. In furtherance of the restrictions on AERO, on January 18, 2018 BIS added the alias "Integrated Solutions" at Lub Thatoo, Hazara Road, The Taxila District, Rawalpindi, Pakistan as an AKA for AERO to the entity list.

11. Effective December 15, 2016, the ERC also added the Pakistan Air Weapons Complex (and six other entities) to the BIS Entity List, writing that they "Have been involved in actions contrary to the national security or foreign policy interests of the United States." And that "Pursuant to § 744.11(b) of the EAR, the ERC determined that the conduct of these seven persons raises sufficient concern that prior review of exports, reexports or transfers (in-country) of items subject to the EAR involving these persons, and the possible imposition of license conditions."

12. I know from my training and experience that Pakistan's unregulated nuclear and Unmanned Aerial Vehicle programs regularly employ a network of individuals and companies in third countries in order to obscure the ultimate end-user of commodities as well as the source of payment for the same. In fact, as part of the addition of AERO to the BIS Entity List, it was published that "Since 2010, Pakistan's AERO has used intermediaries and front companies to procure U.S.-origin items by disguising the end-uses and end-users of the items from U.S. exporters thereby circumventing BIS licensing requirements," and that "AERO has procured items on behalf of Pakistan's Air Weapons Complex, a Pakistani government entity responsible for

[1] As published in The Federal Register on September 19, 2014, 79 FR 55998, pages 55998-56009.

Pakistan's cruise missile and strategic UAV programs."

13. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to the statute. 50 U.S.C. § 1705(a). Willful violations of the EAR constitute criminal offenses under IEEPA, and carry a 20-year maximum term of imprisonment and up to a $1,000,000 fine. 50 U.S.C. § 1705(c). Accordingly, an export that was completed or attempted with the intent that it would be ultimately destined for AERO or the Pakistan AWC would be in violation of IEEPA.

14. I am also aware from my training and experience that entities such as AERO and the Pakistan AWC employ mechanisms by which they obfuscate the source of payments for commodities destined for companies and individuals on the BIS Entity List. Violations of IEEPA are "specified unlawful activities" as defined in 18 U.S.C. § 1956. Therefore, an attempt to "disguise the nature, the location, the source, the ownership, or the control of the proceeds" or transferring funds from outside the United States to inside the United States is violation of the statute.

15. Moreover, some of the information contained in this affidavit comes from my review of the Automated Export System (AES) database maintained by US Customs and Border Protection. AES contains information provided to the United States Department of Commerce in the form of Electronic Export Information (EEI) forms. These forms must be filed by parties to the transaction that are in the United States, such as the seller or shipping company (15 CFR § 30.3), and contain information about all of the parties involved in the transaction. Providing false information, or causing false information to be provided to the United States Department of Commerce on an EEI is a violation of 13 U.S.C. § 205 and 18 U.S.C. § 1001.

PRIOR WARRANT

16. This court, on September 27, 2018, issued a search warrant for Google, Inc. for the contents of these e-mail accounts: industria@gmail.com, buzines@gmail.com, Asad.@gmail.com, business@gmail.com, Buziness@gmail.com, wali.produc@gmail.com, buzinesswo@gmail.com, proc.business@gmail.com, transcoolai@gmail.com, transcoolau@gmail.com, businessintern@gmail.com, magih @gmail.com, proden@gmail.com. Some of the information contained in this affidavit comes from the data returned by Google to me pursuant to this warrant.

FINANCIAL INVESTIGATION

17. Throughout my investigation, businesses in the United States have provided me with information that shipments they sent to Hong Kong, the United Kingdom, Canada and Pakistan have been paid for by "Buziness World" and Haji Wali Muhammad Shiekh of Ontario, Canada.

18. Records maintained by the government of the Province of Ontario, Canada, which I have reviewed, reflect that "Buziness World" is registered in Ontario under Business Identification Number 270217102. Moreover, it is a Sole Proprietorship registered to Haji Wali Muhammad Sheikh of in Mississauga, Ontario. According to employees of the US Department of State with whom I have corresponded, this is a residential address.

19. Two prevalent ways by which money which is exchanged in dollars is transferred between financial institutions are The Clearing House for Interbank Payment Systems (CHIPS) and the Federal Reserve Bank of New York wire services (Fedwire). Pursuant to a grand jury subpoena, both Fedwire and CHIPS provided information to me about money transfers involving

the numerous parties identified as assisting in the unlawful procurement of U.S. origin goods. According to CHIPS, in May and June of 2014, The Canadian Imperial Bank of Commerce account controlled by the Buziness World of , Missisauga, Ontario, Canada received five wire transfers totaling approximately $19,000 USD from an account held by "Director Finance Project 250" ("DFP 250") at the United Bank of Pakistan.

20. The account number at the United Bank of Pakistan for DFP 250 is 20666 . Beginning in July of 2014, this account reflects a name change to "The Business World." Subsequent wire transfers from the account in the name of Business World in Pakistan to Buziness World in Canada continue until at least February of 2017.

21. Fedwire information indicates that Buziness World in Mississauga, Ontario, as well as at 5 Capri Road, Unit 1806 Etobicoke, Ontario (using a Royal Bank of Canada account) have both received funds from The Business World in Rawalpindi, Pakistan using a National Bank of Pakistan account. These wires begin in March of 2015 and continued until at least June of 2017 and totaled approximately $141,953 USD. The funds that were wired out of the Royal Bank of Canada account to US businesses were completed using the name "Haji Wali Muhammad Sheikh" at

22. JP Morgan Chase (JPMC) bank provided me with information about accounts held by "DFP 250" at United Bank of Pakistan and the National Bank of Pakistan. Although DFP 250 is not a customer of JPMC, United Bank of Pakistan maintains a correspondent account with JPMC. According to documents provided to me by JPMC, in March of 2017, DFP 250 received in excess of $5 million USD in two wires from an account at Habib Metropolitan Bank Limited in Pakistan that is held by DFP 250, but which also lists AERO as a holder of the

account. One of the accounts credited was number 20666 at United Bank Limited of Pakistan.

23. Deutsche Bank USA (DBUSA) provided me with information in their possession about accounts held by DFP 250 at banks with which they have a correspondent relationship in Pakistan. DBUSA provided documentation that shows United Bank Limited, Pakistan has account number 20666 registered to DFP 250. However, three transactions in 2014 list the owner of this account as AERO.

24. DBUSA also provided documentation that in April of 2014, DFP 250 used United Bank account number 2066 to transfer $800,000 USD to AERO at Habib Bank in Pakistan. Moreover, DBUSA shows that the address for DFP 250 and AERO at United Bank Limited are all the same: Central Registry, Hazara Road, Hassanabdal, Dist. Attock, Pakistan.

25. Documents from the banks and wire services reflect that AERO, DFP 250, and The Business World in Pakistan all use a registration code of "9010628-8." According to a website maintained by the Pakistani Federal Board of Revenue, this is a "free tax number" assigned to the Pakistan Air Weapons Complex by the Pakistan Federal Board of Revenue. A Free Tax Number is "issued by the Board to persons who are otherwise exempt from holding National Tax Number (NTN) for the purposes of identification." This number was given as part of the account holder information for account number 2066 as late as 2016, which was subsequently retitled to The Business World.

26. Although DFP 250 is not listed on the BIS Entity List, and I have not been able to identify any exports received by DFP 50 in Pakistan or elsewhere, returns from the previous warrant revealed information about them. Specifically, as recently as March 30, 2018 buzines @gmail.com received a purchase order from procuremen @gmail.com for

"Director Finance, Project 250" at Central Registry, Hazara Road, Hassan Abdal, Attock, Pakistan. The phone number listed is 0572-52 and the fax number is 051-9018 This purchase order, number PO-000568-17-18 contains as a line item a pressure gauge made by Ametek Crystal, a company in San Luis Obispo, California. The "Payment Terms" state that: "Payment to M/s Buziness World, Canada / M/s Business International GB Ltf / M/s Business World, Hong Kong / M/s Industria, Hong Kong Ltd / M/s Dutch Tech Engineering B.V M/s Future Tech after receipt and on acceptance of items at Buyer's site against Commercial Invoice through TT in equivalent HKD, RMB or Canadian Dollars."

27. This purchase order also states that the e-mail for DFP 250 is shipment @gmail.com. It also lists as a contact person AHSAN AWAN at 051-4517-4400, and gives an e-mail address for AWAN of logofficer gmail.com

28. A review of other documents shows that on November 23, 2016, Buziness World also received a purchase order from AERO, sent from the e-mail account procurement @gmail.com. The font, layout, and language are the same as that of PO-000568-17-18 from DFP 250. The phone number listed is 0572520522 and the fax is 051-90187228, the same numbers as the PO from DFP 250. The e-mail given for the consignee is shipmen @gmail.com.

29. Also, on January 25, 2016 an e-mail was sent from proc.business @gmail.com to logoffice @gmail.com that contained as an attachment a letter from Faisal Sattar of The Business World in Pakistan to Mr. Ahsan Awan, "AM Logistics" for AERO.

NEW HAMPSHIRE EXPORT TO AERO

30. AES records show that Microdaq.com in Contoocook, NH exported products to "Product Engineering" in Rawalpindi, Pakistan on December 20, 2016. I met with employees of Microdaq who confirmed that they did ship "MCC 100/Dual 50-Pin Hi-Density Cable" valued at 1344 USD and "MCC 16-Channel, 16-Bit Analog Output Board" valued at 5172 USD to this company. The point of contact was Waqar Imran, phone number 9232155 e-mail address proden @gmail.com.

31. Microdaq also provided documentation showing that the payment for this shipment came from the Canadian Imperial Bank of Commerce account maintained by Buziness World.

32. Data provided to me by Google reflects that on July 02, 2015 an e-mail was sent from procurement @gmail.com to buziness @gmail.com that contained "Tender Enquiry" number 000004-15-16 from AERO. This enquiry sought out the exact model numbers and quantity of the products purchased by Product Engineering from Microdaq.com.

33. Subsequently, on May 04, 2016, Purchase Order number 000960-15-16 from AERO was sent from procuremen @gmail.com to buziness @gmail.com for these products and others. This purchase order denotes that payment will be made to "BW Canada."

34. On November 28, 2016 a quote for these products from Microdaq.com was forwarded from prode @gmail.com to bzw @hotmail.com (TA1) and ervices@hotmail.com (TA2). Subsequently a pro forma invoice from Microdaq.com was sent from proden @gmail.com to both b @hotmail.com (TA1) and ervices@hotmail.com (TA2) on December 5, 2016.

35. In turn, on December 7, 2016 a wire report reflecting that Buziness World Canada paid Microdaq.com from their Canadian Imperial Bank of Commerce account was sent from bz @hotmail.com (TA1) to proden @gmail.com.

36. As recently as January of 2018, both bz @hotmail.com (TA1) and services@hotmail.com (TA2) were used to communicate with The Business World in Pakistan regarding the purchase of US commodities.

PRESERVATION OF EVIDENCE

37. On or about May 10, 2018, pursuant to 18 U.S.C. § 2703(f)(1), I sent preservation request letters to Microsoft for bz @hotmail.com (TA1).

38. On October 24, 2018, I again sent a preservation letter to Microsoft for bz @hotmail.com (TA1) and ervices@hotmail.com (TA2).

39. Based on the aforementioned facts, I submit that there is probable cause that the users of the Target Accounts in Pakistan and parties in the United Kingdom, Canada, Hong Kong, Pakistan, and the United States, have acted in furtherance of a conspiracy to purchase US-origin goods for ultimate shipment to entities in Pakistan which are prohibited from receiving US Exports. As such, their actions constitute violations of the Subject Offenses. Accordingly, probable cause exists that evidence of this illegal conduct is present in the Target Accounts.

TECHNICAL BACKGROUND

40. In my training and experience, I have learned that Microsoft provides a variety of online services, including e-mail access, to the public. Microsoft allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the Target accounts. Subscribers obtain an

account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, Microsoft's computers are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. Microsoft e-mail subscribers can access their accounts on servers maintained and/or owned by Microsoft from any computer connected to the Internet located anywhere in the world. E-mail messages and files sent to a Microsoft account are stored in the account's "inbox" as long as they are not identified as "junk mail," the account has not exceeded the maximum storage limit, or the account is not set up to forward messages to another e-mail account. If the message/file is not deleted by the subscriber, the account is below the maximum storage limit, and the account has not been inactivated, then the message/file will remain on the server indefinitely. E-mail messages and files sent from a Microsoft account will remain on the server unless the account user changes the default account settings.

42. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If a Microsoft e-mail user writes a draft message but does not send it, that message may also be saved by Microsoft but may not include all of these categories of data.

43. In my training and experience, in addition to e-mails, Microsoft subscribers can also store files such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Microsoft.

Evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

44. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

LEGAL AUTHORITY

45. The government may obtain both electronic communications and subscriber information from an e-mail provider by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

46. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the website hosting company or e-mail provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

47. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

48. This application seeks a warrant to search all responsive records and information under the control of Microsoft, a provider subject to the jurisdiction of this court, regardless of where Microsoft has chosen to store such information. The government intends to require the

disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. 18 U.S.C. § 2713.

FOURTEEN-DAY RULE FOR EXECUTION OF WARRANT

49. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Microsoft, as with a conventional warrant, but rather by serving a copy of the warrant on the company and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

50. Based on my training and experience and that of other law enforcement, I understand that e-mail providers sometimes produce data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that e-mail providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

51. The United States does not ask for this extra data or participate in its production.

52. Should Microsoft produce late-created data in response to this warrant, I request permission to view all late-created data that was created by Microsoft, including subscriber, IP address, logging, and other transactional data, without further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of

which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail communications, absent a follow-up warrant.

53. For these reasons, I request that the Court approve the procedures in Attachment B, which set forth these limitations.

CONCLUSION

54. Based on the information described above, I have probable cause to believe that records and data from the Target Accounts (as described in Attachment A), contain evidence, fruits, and instrumentalities of the above-listed crimes (as described in Attachment B).

55. The procedures for copying and reviewing the relevant records are set out in Attachment B to the search warrant.

Respectfully submitted

Brendan M. Quinlan
Brendan M. Quinlan
Special Agent
Office of Export Enforcement
Bureau of Industry and Security
United States Department of Commerce

Subscribed and sworn to before me on this 9th day of November, 2018.

/s/ Andrea K. Johnstone
ANDREA K. JOHNSTONE
United States Magistrate Judge

ATTACHMENT A

The premises to be searched and seized are (1) the e-mail accounts identified as bz [redacted]@hotmail.com (TA1) and [redacted]services@hotmail.com (TA2) ("the Target Accounts"), (2) other user-generated data stored with the Target Accounts, and (3) associated subscriber, transactional, user connection information associated with the Target Accounts, as described further in Attachment B. This information is maintained by Microsoft, Inc. ("Microsoft"), which accepts service of process at 1025 La Avenida, Mountain View, California.

ATTACHMENT B

I. Search Procedure

A. Within fourteen days of the search warrant's issue, the warrant will be served on Microsoft, which will identify the accounts and files to be searched, as described in Section II below.

B. Microsoft will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. Microsoft will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Microsoft after fourteen days from the warrant's issue ("late-created data"), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Microsoft without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Accounts and Files to Be Copied by Microsoft Personnel

A. All data files associated with the Target account within the possession, custody, or control of Microsoft, regardless of whether such information is stored, held or maintained inside or outside of the United States, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;

2. The contents of all text or instant messages;

3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;

4. The contents of all calendar data;

5. Lists of friends, buddies, contacts, or other subscribers;

6. Records pertaining to communications between Microsoft and any person regarding the Target Account and any e-mail accounts associated with the Target Account, including contacts with support services and records of actions taken.

B. All subscriber and transactional records for the Target Account and any associated e-mail accounts, including:

1. Subscriber information for these and any associated e-mail accounts:

a. Name(s) and account identifiers;

b. Address(es);

c. Records of session times and durations;

d. Length of service (including start date) and types of service utilized;

e. Telephone instrument number of other subscriber number or identity, including any temporary assigned network address;

f. The means and source of payment for such service (including any credit card or bank account number); and

g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for any connections to or from these and any associated e-mail accounts, including:

a. Connection time and date;

b. Disconnect time and date;

c. The IP address that was used when the user connected to the service;

d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and

e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

A. The items to be seized, which are believed to be evidence and fruits of violations of the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1705; and the Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774; and the Subject Offenses, including an ongoing criminal conspiracy to commit these offenses, 18 U.S.C. § 371, are as follows:

1. Records and information related to violations of the aforementioned statutes and regulations;

2. Records and information related to any purchases, sales, or requests for purchase or sale of suspected U.S.-origin goods or suspected export-controlled items;

3. Records and information related to payments for any U.S.-origin goods or suspected export-controlled items, including bank records, wire transfers, checks, credit card bills, account information, PayPal transactions; other payment websites, or other financial records;

4. Records and information related to any shipping, delivery, or customs declaration of U.S.-origin goods or suspected export-controlled items;

5. Records and information related to actual or potential buyers and sellers of U.S.-origin goods or suspected export-controlled items, including biographical information, addresses, e-mail addresses, user names, social security numbers, or other pertinent identifying information;

6. Records and information related to the identity and whereabouts of any of the individuals or entities associated with the Target Accounts, including biographical information, addresses, e-mail addresses, user names, social security numbers, or other pertinent identifying information;

7. Records and information related to the use or planned use of U.S.-origin goods or suspected export-controlled items;

B. All of the subscriber, transactional, and logging records described in Section II(B).

CERTIFICATE OF AUTHENTICITY

I, _____, attest, under penalties of perjury, that the information contained in this declaration is true and correct. I am employed by Microsoft, Inc., and my official title is _____. I am a custodian of records for Microsoft, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Microsoft, Inc., and that I am the custodian of the attached records consisting of _____ (folders/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Microsoft, Inc.; and

c. such records were made by Microsoft, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature